UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/699,005	10/30/2003	Michael Scheidell	1012-003U	1429

29973 7590 08/22/2007

CAREY, RODRIGUEZ, GREENBERG & PAUL LLP
ATTN: STEVEN M. GREENBERG, ESQ.
950 PENINSULA CORPORATE CIRCLE
SUITE 3020
BOCA RATON, FL 33487

EXAMINER	
SHERKAT, AREZOO	
ART UNIT	**PAPER NUMBER**
2131	

MAIL DATE	DELIVERY MODE
08/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/699,005	SCHEIDELL, MICHAEL	
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 June 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,12,13 and 15-20* is/are rejected.

7)☒ Claim(s) *9-11 and 14* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Response to Amendment

This office action is responsive to Applicant's amendment received on 6/3/2007. Claims 1, 12, and 16 are amended. Claims 1-20 are pending.

Response to Arguments

Applicant's arguments with respect to claims 1-20 have been considered but are moot in view of the new ground(s) of rejection based on newly found references.

Allowable Subject Matter

Claims 9-11 and 14 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-8, 12-13, and 15-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ptacek et al., (U.S. Publication No. 2005/0005017 and Ptacek hereinafter), in view of Lachman, III et al., (U.S. Publication No. 2002/0166063 and Lachman hereinafter).

Regarding claims 1 and 16, Ptacek discloses a computer network intrusion detection system comprising: a plurality of different log analyzers (i.e., ACDs 114-1 through 114-5) for different external networks (i.e., subnet 1- subnet 4), each log analyzer being configured for detecting attacks upon a firewall in a corresponding network defining an edge detection network, an edge database log and coupled to the different log analyzers logging attacks upon the different external networks (i.e., NMM 110 analyzes raw network data, condensing it into a usage model database 115 that describes relationships between network devices which is used as a reference to detect propagation by observing similar deviant behavior on multiple hosts within a short period of time); an intrusion detector coupled to a client network (i.e., ACDs 114-1 through 114-5) and configured to detect external attacks upon the client network (par. 43-47), an analyzer (i.e., ADS 112) coupled to said intrusion detector for analyzing each detected attack and determining a characteristic indicative thereof to classify each detected attack as a general attack (i.e., known attack types) or a [client] specific attack (i.e., unknown attack types) based upon logged attacks in the edge database log (i.e., Ptacek detects two classes of network attacks: a first class of attacks are detected using pattern matching algorithms such as "Snort" system- a second class of attacks, namely "Novel" attacks, are detected using heuristic attack modeling)(par. 74-82); and a filter coupled to said analyzer for generating an alert based upon characteristics of a plurality of attacks (i.e., creating first and second order indications of propagating attacks)(par. 83-95).

Moreover, Lachman discloses an analyzer (i.e., scanner) coupled to said intrusion detector for analyzing each detected attack and determining a characteristic indicative thereof to classify each detected attack as a general attack or a [client] specific attack based upon logged attacks in the edge database log (i.e., specific known attacks and generic policy rules to generate new attack signatures and counter a new unknown attack type – IDS rules or heuristics for a particular type of denial of service attack know as "SYN flood" attack is an example of an IDS policy rule)(col. 5, lines 47-67 and col. 6, lines1-67); and a filter coupled to said analyzer for generating an alert based upon characteristics of a plurality of attacks (i.e., alert generating/reporting actions)(col. 8, lines 40-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Ptacek with teachings of Lachman because it would allow to include an intrusion detector for detecting different classes of attacks as disclosed by Lachman. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Lachman to detect and counter both known and unknown attack types (Lachman, par. 14).

Regarding claim 12, Ptacek discloses a method of generating a network intrusion alert for a first network coupled to a multiple client network system comprising the steps of:

logging attacks on multiple different external networks defining an edge detection network, detecting an attack on a client network (i.e., NMM 110 analyzes raw network data, condensing it into a usage model database 115 that describes relationships between network devices which is used as a reference to detect propagation by observing similar deviant behavior on multiple hosts within a short period of time), classifying the attack as either a general attack or a client specific attack by comparing the attack to attacks logged for the edge detection network (i.e., Ptacek detects two classes of network attacks: a first class of attacks are detected using pattern matching algorithms such as "Snort" system- a second class of attacks, namely "Novel" attacks, are detected using heuristic attack modeling)(par. 74-82); prioritizing handling of the detected attack if the attack is classified as a general (i.e., false positives are ignored and propagating attacks are blocked)(par. 107-113).

Moreover, Lachman discloses an analyzer (i.e., scanner) coupled to said intrusion detector for analyzing each detected attack and determining a characteristic indicative thereof to classify each detected attack as a general attack or a [client] specific attack based upon logged attacks in the edge database log (i.e., specific known attacks and generic policy rules to generate new attack signatures and counter a new unknown attack type – IDS rules or heuristics for a particular type of denial of service attack know as "SYN flood" attack is an example of an IDS policy rule)(col. 5, lines 47-67 and col. 6, lines1-67); and a filter coupled to said analyzer for generating an alert based upon characteristics of a plurality of attacks (i.e., alert generating/reporting actions)(col. 8, lines 40-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Ptacek with teachings of Lachman because it would allow to include an intrusion detector for detecting different classes of attacks as disclosed by Lachman. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Lachman to detect and counter both known and unknown attack types (Lachman, par. 14).

Regarding claim 2, Ptacek discloses the system according to claim 1 wherein said filter generates a first alert signal in response to an attack having a new characteristic, and further generates a second alert signal indicative of a predetermined plurality of attacks having the new characteristic occurring within a predetermined time (i.e., "first order" and "second order" indications)(par. 92-94).

Regarding claim 3, Lachman discloses the system according to claim 1 wherein said filter generates a first alert signal in response to an attack having a new characteristic, and further generates a subsequent first alert signal in response to a subsequent attack having the new characteristic occurring after an absence of attacks having the new characteristic occurring within a predetermined time (i.e., during each cycle, packet sniffing module can collect and analyze twenty packets and then system can sleep a predetermined amount of time assuming that system did not detect an attack ... If the attack is not confirmed, i.e., if the current network load does not exceed

the set load threshold, then the event can be recorded as a warning and the method can branch to step 315 to sleep until the beginning of the next cycle)(par. 86-87 and par. 102-105).

Regarding claim 4, Ptacek discloses the system according to claim 1 wherein said filter generates the alert in response to attacks of a predetermined characteristic exceeding a predetermined rate or frequency (par. 92).

Moreover, Lachman discloses the system according to claim 1 wherein said filter generates the alert in response to attacks of a predetermined characteristic exceeding a predetermined rate or frequency (i.e., if the network load reaches the set threshold, then system can launch a countermeasure routine and con log the time of the flood, the time of the countermeasure deployment, and the source and destination of the offending packets)(par. 105).

Regarding claim 5, Lachman discloses the system according to claim 4 wherein the predetermined rate or frequency deterministically varies (i.e., load threshold can be customized for any network to accommodate different connections based on a percentage of bandwidth capacity of the network)(par. 85).

Regarding claim 6, Ptacek discloses an intrusion detector (i.e., any of the Access Control Devices, ACDs 114-1 through 114-5) for detecting attacks upon a second computer network (i.e., different subnetworks of network 1 – par. 31-35), wherein said

filter (i.e., ADS 112) is further coupled to said second intrusion detector and communicates the alert to the computer network in response to attacks of a predetermined characteristic upon the second computer network exceeding a predetermined rate or frequency (i.e., NMM 110 analyzes raw network data, condensing it into a usage model database 115 that describes relationships between network devices. The ADS 112 uses NMMs covering usage model 115 as a reference for "normalcy" and therefore detects propagation by observing several deviant behavior on multiple hosts within a short period of time)(par. 35-43).

Regarding claim 7, Ptacek discloses further comprising: a vulnerability tester coupled to said analyzer for testing a second computer network for a vulnerability to an attack characteristic detected by said analyzer (i.e., The ADS 112 uses NMMs covering usage model 115 as a reference for "normalcy" and therefore detects propagation by observing several deviant behavior on multiple hosts within a short period of time)(par. 35-43).

Regarding claim 8, Ptacek discloses further comprising: an second intrusion detector for detecting external attacks upon a second computer network; a second analyzer coupled to said second intrusion detector for analyzing each detected attack upon the second network and determining a characteristic indicative thereof, wherein said filter is further coupled to said second analyzer and further compares the attack characteristics determined by said analyzer and said second analyzer and generates a

general attack alert in response to a substantial similarity in the comparison (i.e., the CP 116 receives notifications from the ADS 112 that propagating behavior or other network attack has been identified. The CP 116 then asks NMM 110 for a list of known relationships between network devices that use the same network services as the propagating attack. It combines these two pieces of information to form a recommendation to all ACDs on the network to block traffic)(par. 47-49).

Regarding claim 13, Ptacek discloses the method according to claim 12 further comprising the step of generating a second alert in response to the presence of the match (par. 92-94).

Regarding claim 15, Ptacek discloses the method according to claim 12 wherein said step of determining if the characteristic matches a characteristic of an attack upon a second client determines if the characteristic matches a characteristic of attacks upon multiple clients coupled to the multiple client network system (par. 92-94).

Regarding claim 17, Ptacek discloses the method according to claim 16 further comprising the step of further determining if the characteristic of the attack upon the first host is a new characteristic, wherein said step of testing does not test the susceptibility of the second host if said step of further determining does not determine that the characteristic of the attack upon the first host corresponds to the new characteristic (par. 38-42).

Regarding claim 18, Ptacek discloses the method according to claim 17 wherein the new characteristic corresponds to a characteristic not previously determined (i.e., "Novel" attacks)(par. 81-82).

Regarding claim 19, Ptacek discloses further comprising the step of generating an alert if said step of testing indicates that the second host is susceptible to the determined characteristics (par. 40-44).

Regarding claim 20, Ptacek discloses the method according to claim 16 further comprising the step of filtering the determined characteristics of a plurality of attacks determined by said step of determining and generating an alert signal in response to a substantial increase in frequency or rate of attacks of the characteristic, wherein said step of testing tests the susceptibility of the second host in response to the alert signal (par. Ptacek discloses).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

A.S.
Patent Examiner
Group 2131
August 16, 2007

SYED A. ZIA 08/19/2007
PRIMARY EXAMINER